Data Center Expansion for E-Government of Jordan

Table of Content

1 Technical Management Overview

1.1 Objective

The goal of STS is to partner with the Government of Jordan in helping to ensure and secure a network infrastructure for the E-Government of Jordan Project. The solution should meet the requirements/applications of the Jordan Government and should be accountable to Jordan's overall business strategies and objectives.
The proposed data center solution is around the PIX Firewall and Catalyst 6500 switches; these Cisco's platforms are a key step towards realizing these goals.
Jordan today is evolving their infrastructure to support new business requirements. This includes:

- Web-based services for citizens, connected to the Internet.
- Virtual Private Networks for trusted ministries to access the Data Center via the SGN Network.
- Access for business partners to parts or all of Jordan's E-Government Data Center Network.
- Faster connection for Jordan Online Clients.

The most critical requirement to allow these services is the establishment of a security architecture that protects the resources of E-Government of Jordan, while at the same time allowing users access to the information they require.
This solution proposes Firewall Implementation Services for E-Government of Jordan to enable the PIX Firewall to act as the key security point for connecting the internal Network to the external Internet and to Partners. In addition, the PIX Firewall can act as the key security zone between internal networks that require security services.
The expected benefits include improved authentication, enhanced access control, better information confidentiality and integrity, and improved availability of the network and the attached resources.

1.2 Introduction

The Cisco PIX 535 Firewall is part of the world-leading Cisco PIX Firewall series, providing today's networking customers with unmatched security, reliability, and performance. Ideal for protecting the Data Center's perimeter, the PIX 535 delivers full firewall protection with integrated IP Security (IPsec) virtual private network (VPN) capabilities.

1.3 High Availability

The Cisco PIX Firewall offers unsurpassed reliability, with a mean time between failure (MTB) of more than 60,000 hours. Even with this level of dependability, organizations whose Internet, intranet, or extranet connections are their corporate lifeline know that firewall redundancy is critical. Every minute a firewall is down means lost revenue, opportunity, or critical information.
Cisco has created a failover bundle package for use with the PIX 535, enabling this need to be met simply and inexpensively. This package provides organizations with a second

firewall designed to run exclusively in failover mode, for a fraction of the cost of a standard one.

1.4 PIX Architecture overview

STS offered two Front End firewalls for high availability with three Gigabit Ethernet Interfaces and four FastEthernet interfaces.
The interfaces are distributed as following:

- To connect between the two PIX Firewalls for Stateful failover
- To connect to the Internet zone, a Catalyst 2950 has been provided for such purpose
- The Services zone will be connected with Gigabit Ethernet interface
- The Access zone to SGN Network is connected with FastEthernet interface.
- The Email and Content Management zone is connected with Gigabit Ethernet
- The Front End zone is uplinked with gigabit Ethernet interface

The two Back End firewalls are offered with three Gigabit Ethernet Interfaces and four FastEthernet interfaces.
The used interfaces are distributed as following:

- To connect between the two PIX Firewalls for Stateful failover using Fast Ethernet interface
- The management zone will be connected with Fast Ethernet interface
- The Back End Database zone is connected with gigabit Ethernet interface

1.5 Switching Solution

In the Data Center, we will have five Catalyst 6513 Multilayer switches in the core of the network. The Catalyst 6513 is the flagship of Cisco's high level, layer2 to Layer 7-support switch. The Catalyst 6513 will be configured in a fully redundant fashion with Dual Power Supplies and two Supervisor engines and two MSFC-2. The fans and network clocks will also be redundant. The Switching Fabric Module will be included in the chassis to scale the throughput of the backplane from 32Gbps to 256Gbps.

For the server aggregation we will have all the servers connected directly with Gigabit Ethernet to the catalyst 6513 switches. These servers will have dual-homed connectivity to the core switches to increase the availability for the critical servers.

As you can see from the architecture above, we have designed the E-Government of Jordan's network around Cisco's 6513 platforms that will play a key role in network stability and throughput. Cisco's IOS contains a mature set of features that have been carefully refined over many years by Cisco and our customer's real world experience. The Government of Jordan's data center is well served by the Catalyst 6513's and Catalyst 2950 impressive list of features and performance.

The Catalyst 2950 series of switches are proposed for external segment. The Catalyst 2950 series is the highest capacity and most cost effective stickballs in the industry today; they are equipped with a 13.6Gbps fabric and can boost over 7.5 million packets per

second in performance. No competitor comes close to matching the flexibility and performance of the Catalyst 2950 series. The Catalyst 2950 does not spare any rich feature either, it fully supports all the requirements for data center, including Security, QoS, Multicast, Resiliency and high performance/bandwidth.

The Catalyst 6500 is Cisco's high end Gigabit Ethernet and Server aggregation switch. It has an unmatched density for up to 130 Gigabit Ethernet ports and supports 32Gbps backplane scalable to 256G. The Catalyst 6500 supports L2-L7 services starting with basic Layer 2 and 3 support, moving to Layer 4 services such as extended Security and QoS, and moving to L4-7 with support for Server Load Balancing and Web Caching/URL filtering. It also supports the PFC (Policy Feature Card), which provides policy networking enforcement at wire speed on all ports.

1.6 E-Government and Web-Scaling

The Cisco Content Switching blade integrated within the Cat6513 enables Government of Jordan engaged in e-business to build global Web networks optimized for e-business transactions and Web content delivery. With its patented content switching technology, the Content switching gives businesses maximum control in ensuring availability of Government of Jordan Web site, securing Web site resources without compromising performance, and allocating Web site resources efficiently.

The content switch is provided to build and scale with the Intranet, extranet and Internet connection for the future. The Content switching blade is suggested in the Services Zone and in the Content Management zone. On those segments, we have a similar design where we are including two Content switching blades connected together back to back or within the same chassis as per the Services zone; running VRRP in between each other with NAT hiding the real IP from outside, these blades are capable of DOS attacks prevention and content awareness.

Benefits of the Content Switching blades:

- Provides high-speed Web content delivery by selecting the best site and server based on full URL, cookie, and resource availability information
- Offers site-level security with wire-speed denial-of-service (DoS) prevention; firewall load-balancing provides scalable security for web servers
- Delivers up to 400 percent improvement in Web cache efficiency for transparent, proxy, and reverse proxy configurations
- Supports all TCP- and UDP-based Web protocols, wire-speed network address translation (NAT), and integrated IP routing
- Optimizes both content requests and delivery for HTTP, passive File Transfer Protocol (FTP), and streaming media protocols
- Enables advanced service level agreements (SLAs), and a variety of new fee-based services

Featuring patented content-switching technology, Cisco Content switching blade gives Government of Jordan businesses maximum control in allocating e-business site resources and building services for optimal return on investment (ROI). By implementing

Content Switching Network Services for e-business, Government of Jordan their hosting partners/Ministries can provide reliable, secure, high-performance e-government sites that are continuously "open for business."

1.7 Internal Network Security

According to FBI, 80% of the attacks are from the internal users; hence, STS's consultant suggests using an intrusion detection system IDS.

We included in our Solution three more IDS's. One located on the external segment , one located on the SGN segment one in the CMS, and one in the Front End Servers Zone; excluding the SGN & Internet IDS's, the other two IDS's can be moved to monitor the Various segments, to create a baseline for the internal segments.

These IDS have the following features listed below.

Sophisticated Attack Detection and Antihacking Protection:

- *Exploits*—Activity indicative of someone attempting to gain access or compromise systems on your network, such as Back Orifice, failed login attempts, and TCP hijacking
- *Denial-of-service (DoS)*—Activity indicative of someone attempting to consume bandwidth or computing resources to disrupt normal operations, such as Trinoo, TFN, and SYN floods
- *Reconnaissance*—Activity indicative of someone probing or mapping your network to identify "targets of opportunity," such as ping sweeps and port sweeps; usually a precursor to an actual exploit attempt
- *Misuse*—Activity indicative of someone attempting to violate corporate policy; this can be detected by configuring the sensor to look for a custom text strings in the network traffic; for example, XYZ Corporation could easily configure the Cisco Secure IDS to send an alarm on and eliminate any connection that transmits the phrase "XYZ Confidential" in e-mail or File Transfer Protocol (FTP)
- Real-time capability, as opposed to a periodic review of log files, can significantly reduce potential attack damage and recovery costs by eliminating a hacker from the network
- By presenting decision-critical intrusion alarm information, such as offending and destination IP addresses, destination port, and attack descriptions, users can develop metrics and track trends to determine the security state of a network
- Information can be ported to a relational database and provide the basis for more accurate, fact-based decision-making regarding the security of the network

1.8 Management Solution

We are providing CiscoSecure Access Control Server, which includes Radius and TACACS+. This Authentication, Authorization and Accounting software will help E-Government of Jordan to authenticate against any connection from inside to outside or outside to inside and it is highly advisable to be used with the VPN concentrators and for

VPN Clients. Unlimited number of VPN Clients license will be delivered part of this solution with zero Dollar value.

The CiscoSecure VPN/Managed Services will include CiscoSecure Policy Manager, which will help firewall administrators to manage and enforce policies on the PIX Firewall through a GUI Interface eliminating the need to handle the IOS commands. As well, the CSPM is used to manage the Intrusion Detection System's Signatures and attacks Database monitoring.

1.9 Design Summary

As you can see from the architecture above, we have designed E-Government of Jordan's network around Cisco's platforms that will play a key role in network stability and throughput. Cisco's IOS contains a mature set of features that have been carefully refined over many years by Cisco real world experience. E-Government of Jordan's network is well served by Cisco Product impressive list of features and performance .

2 Design Building Blocks

In the Data Center Design, there have been some modification between the Items proposed in phase I and Phase II in the project, taking several aspects of the Data Center into Consideration, some of these considerations may intercept across the Data Center, the design has taken into confederations the following issues:

- Security
- Redundancy
- Highavailability
- Performance
- Scalability
- Future growth

2.1 Security

Network Security is one of today's biggest challenges for leading edge enterprises. The primary factor driving this security challenge is the Internet. With the demands by customers for increased electronic commerce and web-based client services comes the threat of increased vulnerability through unauthorized access.

The eGov. Is a major victim of such attacks, hence a security policy should be enforced, STS Focused network security solutions team has developed the STS methodology and Security Circle that involves :

1. Network Probing & Vulnerability Assessment of the existing Network
2. Security Policy Consulting & Security Solutions Design & Implementing
3. Security Operations Support
4. Security policing and Monitoring
5. And the Cycle is repeated.

Based on the above network as well as physical security are issues, and based on the nature of the eGovernment operations, and criticality, Physical separation between segments and devices were introduced in the design.

2.2 Redundancy & Highavailability

As more and more critical applications move on the Internet & SGN providing highly available services becomes increasingly important. A major requirement is having hardware and software redundancy. High availability can be provided by detecting node or daemon failures and reconfiguring the system appropriately so that the workload can be taken over by the remaining nodes in the cluster.

In fact, high availability is a big field. An elegant highly available design may include online high availability in network equipment & servers, as well as offline ready to run equipment that just needs to be powered on.

In the network design; Box redundancy was introduced, as well as power redundancy on some boxes, redundant power supplies, Controllers, and Cards were introduced were applicable, as well as box redundancy running Host Standby, Dual Homing and Failover architectures.

A recommendation for further guaranteeing high availability was made to supply the redundant power supplies and redundant boxes with power from a different power source, supported by different UPS sets and Power generators.

2.3 Performance, Scalability & Future Growth

The current setup & design of the Data Center & SGN networks will initially serve six pilot ministries with an email system only and some web application. With a plan to eventually connect up to 126 ministries & governmental departments and offices with a total of around 120,000 users in the G2G environment only.

Not neglecting the number of G2C & G2B connections, which might rise up if not larger than the number of the Government network users.

The applications, services & procedures will also emerge and grow in functionality and number, the database of all the applications and information will also grow exponentially once the service is launched, all these factors were taken into consideration when designing the Data Center, so a scalable upgradeable design approach was taken, as well as offloading servers from unnecessary functions that can be performed by appliance base H/W.

3 The Architecture Components

In the network design, various Cisco technologies and devices were used providing cutting edge technology and performance. The following equipment were used

- Cisco 7200 Routers
- Cisco 7100 Routers
- Catalyst 6513 Switches
- Catalyst 2950 Switches
- Cisco Secure PIX 535
- Cisco Secure IDS

3.1 Cisco 7200

Two Cisco 7200 routers were introduced in the SGN segment of the Data Center to provide connectivity with pilot ministries; redundancy & performance were the major factors in selecting the 7200 router. As it offers on box power supply redundancy as well as running Hot Standby Routing Protocol (HSRP) between the two routers, one will be connected to the leased line connections while the other will be handling the dial backup traffic.

The scalability issue was also addressed when selecting the 7200 router, as it supports STM1 interfaces with a bandwidth of 63 E1's & 256 Channel groups, which is more than the actual number of the final connected SGN centers. Naturally this is dependant on the availability of the lines / interfaces from the carrier; which is JT.

A third Cisco 7200 was introduced for the internet setup, with a redundant power supply, only one 7200 was introduced here, as there is only one link to the internet at this stage, another router should be added when an increase in bandwidth, or link is introduced.

3.2 Cisco 7100

The Cisco 7100 was introduced in the second phase of the project to replace the VPN3030, which was introduced in phase I to terminate the VPN tunnels from the remote users and the pilot six ministries, and to be relocated in later phases to only terminate the VPN client remote users .

The 7100 hundred was to be placed in the design in a later phase to terminate all the site to site VPN's between the ministries and the Data Center, however as the remote access was removed from phase 1, The 7100 was introduced in this phase of the project, as it better handles multiple VPN sessions, as will as ease of management and routing issue between the various segments of the network.

Again, the 7100 answers to the redundancy, performance and highavailability conditions as the Cisco 7200 in addition to the security aspect of the setup

3.3 Catalyst 6513 & Catalyst 2950

The Catalyst 6513 was introduced as it is the flagship of Cisco enterprise switching solutions, providing high availability, performance, scalability and upgradeablility, the 6513 was introduced with various scenarios in different segments, and in the current setup for the Data Center, five Boxes were introduced.

Physical separation between the boxes were introduced between boxes in different security zones, this physical separation includes installation in different communication cabinets, this was to cover the security constrains in the design.

High availability was also a major factor in the design, as two CAT 6513 were introduced in the Back end and Front end Segments, catering for power supply redundancy, supervisory redundancy on the same Box, plus box redundancy, providing highavailability and load balancing. the CMS segments has only one fully redundant switch with a recommendation to duplicate the box physically in a later phase.

The Cat 6513 was proposed over the Cat6506 and the Cat 6509 as the Cost in the chassis was negligible, thus providing higher range of upgradability and scalability in the future as it provides a 13 slot chassis. Other scalability issues were that the Cat 6500 is a layer 3-7 switch, with Content, IDS, firewall, IP telephony, flex WAN & 10 Gigabit modules available in the market now, and development is still proceeding to introduce more fixable and provide more functionality to this box.

Performance was also a major factor in choosing the Cat6500 family, as it can scale up to 256G in switching capability with a forwarding rate of up to 210Mpps.

The cat6513 with a two content blades was introduced in the CMS segment, as gigabit interfaces were required for the server connectivity, as well as the performance issues on the Cat6500 versus the standard content switches. The content blade was introduced to offload the servers from the load balancing hassle, thus offloading the CPU and memory of the server, and catering for better response and performance for the end customer.

The Catalyst 2950 was introduced in the outer segment of the Data Center to cater for the Issue of security and physical separation between the various segments of the Data Center.

3.4 Cisco Secure elements (PIX & IDS)

The PIX firewall 535 was introduced to cater for security and performance, the PIX 535 is the top of the line in Cisco Secure firewall Family, equipped with redundant power supplies and running in Failover mode, the PIX 535 also answers the redundancy and highavailability constraint.

The Pix 535 was chosen over the PIX blade in the Catalyst 6500, as physical separation is an issue for security. The PIX 535 is equipped with 10 PCI slots that can be populated with Gigabit, 10/100 Quad , 10/100 Single & VPN accelerator Cards.

The Cisco Secure IDS was introduced as part of the STS security wheel, which included policing and securing the network, the IDS answers to the security constraint of the design, however the IDS was chosen over the IDSM in the Cat 6500 for the outer segments, as automatic response to certain attackes are required, these responses include

- TCP reset
- IP Blocking
- Packet logging

Out of which only the third is being supported by the IDSM.

3.5 Cisco Secure Content Accelerator

The Cisco Secure Content Accelerator has been introduced in the CMS segment of the data center to address the issues of security & performance.

Security as all the SSL tunnels will be terminated on this device, offloading the servers, and load balancing between the various servers, (performance).

Another factor is that only one digital certificate for all the connected servers would need to be downloaded on each client machine.